

Polynômes en une variable : racines, corps de décomposition, extensions de corps

Marc Abboud

27 Janvier 2021

1 Résultats sur les corps

1.1 L'anneau des polynômes $\mathbf{K}[X]$

Soit \mathbf{K} un corps, on peut définir l'anneau des polynômes $\mathbf{K}[X]$ et on sait que cet anneau est euclidien, il est donc principal et donc factoriel. Soit A une \mathbf{K} -algèbre, pour définir un morphisme de \mathbf{K} -algèbre $\mathbf{K}[X] \rightarrow A$ il faut et il suffit de définir l'image de X (Cette propriété caractérise l'anneau $\mathbf{K}[X]$).

Proposition 1.1. *Soit A un anneau principal et a un élément non nul de A . Les propriétés suivantes sont équivalentes :*

1. *L'idéal (a) est premier, c'est à dire que le quotient $A/(a)$ est intègre ;*
2. *a est irréductible ;*
3. *L'idéal (a) est maximal ; c'est à dire que le quotient $A/(a)$ est un corps.*

Exercice 1. Donner un critère simple pour savoir si un polynôme de degré ≤ 3 est irréductible dans $\mathbf{K}[X]$.

1.2 Caractéristique d'un corps

Soit \mathbf{K} un corps, il existe un plus petit sous-corps de \mathbf{K} appelé *sous-corps premier de \mathbf{K}* . C'est le corps engendré par 1. Plus précisément, il existe un unique morphisme d'anneaux $\mathbf{Z} \rightarrow \mathbf{K}$ défini par

$$\varphi : n \in \mathbf{Z} \mapsto n \cdot 1_{\mathbf{K}} \in \mathbf{K}$$

De deux choses l'une ;

1. Ou bien ce morphisme est injectif et dans ce cas le sous-corps premier de \mathbf{K} est isomorphe à \mathbf{Q} , on dit que \mathbf{K} est de *caractéristique nulle*.
2. ou bien le noyau du morphisme est de la forme $n\mathbf{Z}$, comme le quotient est un sous-anneau de \mathbf{K} c'est un anneau intègre donc n est un nombre premier que l'on note p . C'est la *caractéristique* de \mathbf{K} . Le sous-corps premier de \mathbf{K} est alors isomorphe à $\mathbf{Z}/p\mathbf{Z}$ que l'on note \mathbf{F}_p .

Exercice 2. Soit \mathbf{K} un corps de caractéristique $p > 0$, montrer que le morphisme de Frobenius

$$x \in \mathbf{K} \mapsto x^p$$

est un morphisme de corps.

1.3 Extension de corps

Proposition 1.2. Soit \mathbf{K} un corps, tout morphisme d'anneaux $\mathbf{K} \rightarrow A$ est injectif.

On appelle extension de corps tout morphisme d'anneaux $\mathbf{K} \hookrightarrow \mathbf{L}$ avec \mathbf{K} et \mathbf{L} des corps, \mathbf{L} hérite alors d'une structure de \mathbf{K} -espace vectoriel et on dit que l'extension est *finie* si \mathbf{L} est de dimension finie sur \mathbf{K} . On appelle *degré de l'extension* la dimension de \mathbf{L} sur \mathbf{K} et on le note $[\mathbf{L} : \mathbf{K}]$.

On dit qu'une extension est de *type fini* si elle est engendrée par un nombre fini d'éléments. C'est à dire qu'il existe un nombre fini d'éléments $\alpha_1, \dots, \alpha_l$ tel que $\mathbf{L} = \mathbf{K}(\alpha_1, \dots, \alpha_l)$. On dit que l'extension est *monogène* si elle est engendrée par un seul élément.

Proposition 1.3 (Multiplicativité des degrés). Soit $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$ une tour d'extensions de degrés finis. On a

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}]$$

Exercice 3. Soit \mathbf{K} un corps, $x, y \in \mathbf{K}$ et une extension de corps $\mathbf{K} \hookrightarrow \mathbf{L}$ tel que \mathbf{L} contienne \sqrt{x}, \sqrt{y} . Montrer que $[\mathbf{K}(\sqrt{x}, \sqrt{y}) : \mathbf{K}] = 4$ si et seulement si x, y et xy ne sont pas des carrés dans \mathbf{K} .

Exercice 4. Soit \mathbf{K} un corps de caractéristique $\neq 2$, montrer que toute extension de degré 2 sur \mathbf{K} est de la forme $\mathbf{K}(\sqrt{x})$ pour $x \in \mathbf{K}$.

1.4 Éléments algébriques et transcendants d'une extension

Soit $\mathbf{K} \subset \mathbf{L}$ une extension de corps. On dit qu'un élément α de \mathbf{L} est *algébrique* sur \mathbf{K} s'il est racine d'un polynôme non nul à coefficients dans \mathbf{K} . Un élément qui n'est pas algébrique est appelé *transcendant*. On dit que \mathbf{L} est algébrique sur \mathbf{K} si tous ses éléments le sont.

Soit $\alpha \in \mathbf{L}$, la sous \mathbf{K} -algèbre de \mathbf{L} engendrée par α est l'image du morphisme de \mathbf{K} -algèbres

$$\text{ev}_\alpha : P \in \mathbf{K}[X] \mapsto P(\alpha) \in \mathbf{L}$$

Théorème 1.4. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension de corps et α un élément de \mathbf{L} .

1. Si α est transcendant sur \mathbf{K} , alors ev_α est injectif, le corps engendré par α est alors isomorphe à $\mathbf{K}(X)$.
2. Si α est algébrique sur \mathbf{K} , alors le noyau de ev_α est un idéal maximal de $\mathbf{K}[X]$, on note P_α l'unique générateur unitaire de $\ker \text{ev}_\alpha$. C'est un polynôme irréductible sur \mathbf{K} qu'on appelle le polynôme minimal de α sur \mathbf{K} , $\mathbf{K}[\alpha]$ est alors un corps isomorphe à $\mathbf{K}[X]/(P_\alpha)$. C'est une extension finie de \mathbf{K} .

On a en fait les équivalences : α est algébrique sur $\mathbf{K} \Leftrightarrow \mathbf{K}[\alpha]$ est de dimension finie sur $\mathbf{K} \Leftrightarrow \mathbf{K}[\alpha]$ est un corps.

Corollaire 1.5. Toute extension finie est algébrique. Toute extension engendrée par un nombre fini d'éléments algébriques est finie, donc algébrique.

Corollaire 1.6. Toute extension engendrée par des éléments algébriques est algébrique.

Théorème 1.7. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension de corps. L'ensemble des éléments de \mathbf{L} algébriques sur \mathbf{K} est un sous-corps de \mathbf{L} contenant \mathbf{K} . C'est la clôture algébrique de \mathbf{K} dans \mathbf{L} .

Proposition 1.8. Soit $\mathbf{K} \hookrightarrow \mathbf{L} \hookrightarrow \mathbf{M}$ une tour d'extension et $x \in \mathbf{M}$. Si x est algébrique sur \mathbf{L} et que \mathbf{L} est algébrique sur \mathbf{K} , alors x est algébrique sur \mathbf{K} .

Exercice 5. C'est faux si on n'a pas un sous-corps sur lequel tout le monde est algébrique. Prenons $\mathbf{K} = \mathbf{Q}(T), \mathbf{K}_1 = \mathbf{Q}(T^2), \mathbf{K}_2 = \mathbf{Q}(T^2 - T)$. Montrer que \mathbf{K} est algébrique sur \mathbf{K}_1 , sur \mathbf{K}_2 mais que \mathbf{K} n'est pas algébrique sur $\mathbf{K}_0 = \mathbf{K}_1 \cap \mathbf{K}_2$.

On dit qu'un corps \mathbf{K} est algébriquement clos si tout polynôme de $\mathbf{K}[X]$ a une racine dans \mathbf{K} . Une *cloture algébrique* de \mathbf{K} est une extension $\mathbf{K} \hookrightarrow \mathbf{L}$ algébrique telle que \mathbf{L} est algébriquement clos.

Théorème 1.9. Soit \mathbf{K} un corps, alors \mathbf{K} admet une clôture algébrique. Deux clôtures algébriques sont isomorphes en tant que \mathbf{K} -algèbre.

Exercice 6. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension de corps avec \mathbf{L} algébriquement clos, montrer que la clôture algébrique de \mathbf{K} dans \mathbf{L} est une clôture algébrique de \mathbf{K} .

Exercice 7. Montrer que si \mathbf{K} est dénombrable, alors $\overline{\mathbf{K}}$ est dénombrable, en déduire qu'il existe des nombres réels transcendants sur \mathbf{Q} .

Exercice 8. (Dur) Montrer que la clôture algébrique de \mathbf{F}_p est

$$\overline{\mathbf{F}_p} = \bigcup_{k \geq 1} \mathbf{F}_{p^k}$$

2 Polynômes et racines

On va maintenant partir d'un polynôme sur un corps \mathbf{K} et trouver des corps plus gros dans lesquels ce polynôme a des racines.

2.1 Corps de rupture

Definition 2.1. Soit K un corps et P un polynôme irréductible. On appelle *corps de rupture* tout élément minimal pour l'inclusion parmi les extensions de corps $\mathbf{K} \hookrightarrow \mathbf{L}$ qui contiennent une racine de P .

Proposition 2.2. Tout corps de rupture de P est isomorphe à $\mathbf{K}_P := \mathbf{K}[X]/(P)$.

Démonstration. Soit \mathbf{L} un corps de rupture et $\alpha \in \mathbf{L}$ une racine de P . Le morphisme d'évaluation $\text{ev}_\alpha : \mathbf{K}[X] \rightarrow \mathbf{L}$ a pour image $\mathbf{K}[\alpha]$ et est un corps. Par minimalité on a que $\mathbf{K}[\alpha] = \mathbf{L}$. \square

Proposition 2.3. Soit \mathbf{K} un corps et P un polynôme irréductible de degré d , alors $\mathbf{K}[X]/(P)$ est une extension finie de \mathbf{K} de degré d .

Proposition 2.4. Soient $\mathbf{K} \hookrightarrow \mathbf{L}$ et $P \in \mathbf{K}[X]$ un polynôme irréductible, pour toute racine $\alpha \in \mathbf{L}$ de P , il existe un unique morphisme de \mathbf{K} -algèbre $\mathbf{K}_P \hookrightarrow \mathbf{L}$ qui envoie X sur α .

Corollaire 2.5. Soit \mathbf{K} un corps et $\mathbf{L} = \mathbf{K}(x)$ avec x algébrique sur \mathbf{K} et Ω une clôture algébrique de \mathbf{K} . Soit $\sigma : \mathbf{K} \hookrightarrow \Omega$ un plongement de \mathbf{K} dans sa clôture algébrique, montrer que σ s'étend à \mathbf{L} et qu'il y a autant de prolongements que de racines distinctes du polynôme minimal de x dans Ω .

Corollaire 2.6. En déduire que le corollaire précédent est encore vraie si l'extension $\mathbf{K} \hookrightarrow \mathbf{L}$ est finie.

2.2 Corps de décomposition

On dit qu'un polynôme est scindé s'il s'écrit comme produit de polynômes de degré 1.

Théorème 2.7. Soit \mathbf{K} un corps et $P \in \mathbf{K}[X]$.

1. Il existe une extension $\mathbf{K} \hookrightarrow \mathbf{L}$ dans laquelle P est scindé, de racines x_1, \dots, x_d telle que $L = \mathbf{K}(x_1, \dots, x_d)$.
2. Deux telles extensions sont isomorphes.

Une telle extension s'appelle un *corps de décomposition* de P .

Exercice 9. Soit $P = X^3 - 2 \in \mathbf{Q}[X]$, montrer qu'un corps de décomposition de P est $\mathbf{Q}(\sqrt[3]{2}, j)$. Montrer que c'est une extension de degré 6.

2.3 Extension séparable

Definition 2.8. Soit \mathbf{K} un corps et f un polynôme de $\mathbf{K}[X]$. On dit que f est *séparable* si f est scindé à racines simples sur une clôture algébrique de \mathbf{K} . Dans le cas contraire, on dira qu'il est *inséparable*.

Lemma 2.9. Un polynôme P est séparable si et seulement si $P \wedge P' = 1$.

Lemma 2.10. Un polynôme irréductible $P \in \mathbf{K}[X]$ est séparable si et seulement si $P' \neq 0$. Il est inséparable si et seulement si la caractéristique p de \mathbf{K} est non nulle et si $P \in \mathbf{K}[X^p]$.

Lemma 2.11. Soit \mathbf{K} un corps de caractéristique $p > 0$ et $a \in \mathbf{K}$ telle que a ne possède pas de racines p -ièmes dans \mathbf{K} , alors le polynôme $X^p - a$ est irréductible sur \mathbf{K} et inséparable.

Definition 2.12. Un corps \mathbf{K} est parfait si tout polynôme irréductible de $\mathbf{K}[X]$ est séparable.

Proposition 2.13. Tout corps de caractéristique nulle est parfait. Tous les corps finis sont parfaits.

Definition 2.14. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension algébrique et soit $a \in \mathbf{L}$. On dit que a est séparable sur \mathbf{K} si le polynôme minimal de a l'est. On dit qu'une extension est séparable si tous ses éléments le sont.

Definition 2.15. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension finie et $\sigma : \mathbf{K} \hookrightarrow \Omega$ un plongement de \mathbf{K} dans une clôture algébrique Ω de \mathbf{K} . On définit le *degré séparable de \mathbf{L} sur \mathbf{K}* que l'on note $[\mathbf{L} : \mathbf{K}]_s$ le nombre de prolongement de σ à Ω .

Proposition 2.16 (Multiplicativité des degrés séparables). Soit $\mathbf{K} \hookrightarrow \mathbf{L} \hookrightarrow \mathbf{M}$ une tour d'extension. On a

$$[\mathbf{M} : \mathbf{K}]_s = [\mathbf{M} : \mathbf{L}]_s [\mathbf{L} : \mathbf{K}]_s$$

Proposition 2.17. Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension finie, on a

$$1 \leq [\mathbf{L} : \mathbf{K}]_s \leq [\mathbf{L} : \mathbf{K}]$$

avec égalité si et seulement si l'extension est séparable.

Proposition 2.18. Si $\mathbf{K} \hookrightarrow \mathbf{L}$ est une extension algébrique engendrée par une famille $(\alpha_i)_{i \in I}$, alors \mathbf{L} est séparable sur \mathbf{K} si et seulement si les α_i sont séparables sur \mathbf{K} .

Théorème 2.19 (de l'élément primitif). Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension de corps telle que $\mathbf{L} = \mathbf{K}(x, y_1, \dots, y_n)$ où les y_i sont séparables sur \mathbf{K} , alors il existe $z \in \mathbf{L}$ telle que $\mathbf{L} = \mathbf{K}(z)$.

3 Résultats à connaître

Proposition 3.1. Un polynôme est irréductible dans $\mathbf{Q}[X]$ si et seulement si il est irréductible dans $\mathbf{Z}[X]$.

Théorème 3.2 (Critère d'Eisenstein). Soit p un nombre premier et $P = a_0 + a_1X + \dots$ unitaire tel que p divise tous les a_i et p^2 ne divise pas a_0 . Montrer que P est irréductible sur $\mathbf{Z}[X]$.

Exercice 10. En déduire qu'il existe des polynômes irréductible de degré arbitrairement grand dans $\mathbf{Q}[X]$, en déduire que l'extension algébrique $\mathbf{Q} \hookrightarrow \overline{\mathbf{Q}}$ est infinie.

Proposition 3.3 (Invariance du PGCD par extension de corps). Soit $\mathbf{K} \hookrightarrow \mathbf{L}$ une extension de corps et $f, g \in \mathbf{K}[X]$. On a

$$f \wedge_{\mathbf{K}[X]} g = f \wedge_{\mathbf{L}[X]} g$$

3.1 Lemme de Gauss et irréductibilité dans $\mathbf{Z}[X]$

Soit $f \in \mathbf{Z}[X]$, le *contenu* de f est le pgcd de ses coefficients, on le note $c(f)$. On dit qu'un polynôme est primitif si son contenu vaut 1.

Proposition 3.4 (Lemme de Gauss). Soient $f, g \in \mathbf{Z}[X]$, alors $c(fg) = c(g)c(f)$.

Proposition 3.5. Soient $P, Q \in \mathbf{Z}[X]$ avec P primitif et $R \in \mathbf{Q}[X]$ tel que $Q = PR$, alors $R \in \mathbf{Z}[X]$.

Théorème 3.6. Soit $f \in \mathbf{Z}[X]$ f , alors si f est irréductible dans $\mathbf{Z}[X]$, il est irréductible dans $\mathbf{Q}[X]$.

La source de ce texte est le poly d'Algèbre 2 d'Olivier Debarre.